For critical infrastructure protection efforts to come even close to being successful, federal, state and local governments and private industry have specific roles and functions that must be integrated.

Developing a Defense

States' role in protecting critical infrastructures is still emerging

By Barry Hopkins

After the terrorist attacks of Sept. 11, the concept of "critical infrastructure" took on new meaning and received a new level of attention. More than two years later, states and the federal government are still ironing out the details of how to work together with local governments and with the private sector to protect the nation's infrastructure.

The USA Patriot Act defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters."

The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, released in February 2003, defines specific sectors as critical infrastructures under the guidelines of the USA Patriot Act. These sectors include agriculture and food, water, public health, emergency services, the defense industrial base, government, telecommunications/information systems, energy, transportation, banking and finance, the chemical industry, and postal and shipping.

The United States' critical infrastructures are a highly diverse, interdependent mix of facilities and networks. Failure in one infrastructure can cascade to cause disruption or failure in others, and the consequences for states and the public can be massive.

Protecting critical infrastructure is a complex mission that involves a broad range of functions performed throughout government and the private sector. Although governments own and operate some of these facilities, most are controlled by the private sector. Much of the expertise required to plan for and ensure the protection of critical infrastructures, therefore, lies outside of the federal government, including much of the knowledge about what needs to be protected. In effect, responsibility for defending critical infrastructures is shifted down to state and local governments and private sector stakeholders.

Because infrastructure protection encompasses such a broad scope, it is foolish to think we can fully protect everything; therefore our strategy must also include national preparedness and response. This combined focus – critical infrastructure protection and incident response – encompasses activities related to national defense, law enforcement, transportation, emergency management, food safety, public health, information technology and other areas. For critical infrastructure protection efforts to come even close to being successful, federal, state and local governments and private industry have specific roles and functions that must be integrated.

New Regulations Raise Questions

In February, the Department of Homeland Security issued new regulations that will allow the federal government to collect sensitive data about physical and cyber infrastructure while allowing this information to remain secret. While no doubt this data will prove vital in efforts to protect our nation's critical infrastructure, questions remain about how it will be shared with states and how states will fit into future critical infrastructure protection efforts.

The new regulations launched the Protected Critical Infrastructure Information program, which, according to Department of Homeland Security, will allow the government to protect the proprietary data of private sector companies, thereby facilitating their voluntary participation in protecting infrastructure.

The information will be exempt from the Freedom of Information Act and will not be accessible by state and local governments for litigation purposes. This raises concerns that companies could submit false information to states to escape prosecution and investigation of their activities.

More importantly, however, from the standpoint of homeland security, it raises questions about whether or not state officials will have access to this information and what role they will play in future protection efforts.

The Council of State Governments recently published a *State Official's Guide to Critical Infrastructure Protection*. According to the guide, state responses to critical infrastructure protection have so far been somewhat limited, in part because of the lack of information sharing among various levels of government and the private sector. Other factors include the fact that infrastructure protection is still a relatively new concept, a tendency to focus more on responding to events than preventing them, and state budget problems.

The guide outlines the challenges associated with protecting the various sectors, what states are currently doing, and strategies states can take to improve their critical infrastructure protection efforts.

To order a copy of the guide, visit our online store at *www.csg.org* (keyword: store) or call (800) 800-1910.

— Barry Hopkins is chief infrastructure policy analyst at The Council of State Governments.